ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

Section I

This warrant authorizes the search and seizure of the items identified in Section I from the locations identified in Attachment A:

1. Any and all sports memorabilia to include, but not limited to, baseball, football, and hockey cards, and pennants.

2. Financial records, including bank statements, credit card statements, tax returns, ledgers, and other documents that indicate banks utilized or possessed by KENNERT, and that detail the sale, possession, creation, importation, and/or purchase of counterfeit sports memorabilia, coins, currency or other counterfeit items;

3. Machines, inks, presses, or other tools that could be used to create counterfeit sports memorabilia or other counterfeit to include instructions and/or directions.

4. Contacts of other counterfeiters, co-conspirators and/or unknown victims to include names, phone numbers, email addresses and physical addresses.

5. Mailing labels, shipping envelopes, and other items used to ship items sold online;

6. Documents or other items concerning residence, occupancy or ownership of the subject premise or vehicles;

7. Any documents concerning ownership, use, or control of storage units or other locations where evidence may be stored;

8. Any safes, locked cabinets, or other secured containers, which officers shall be permitted to open by force or through the use of a locksmith if necessary

9. Any documents or files that detail false or stolen identities, businesses associated with these identities and/or KENNERT as well as financial records associated with these;

10. Any computer, computer system, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, data disks, system disk operating systems, magnetic media floppy disks, Internet-capable devices, cellular telephones, tablets, digital music players, hardware and software operating manuals, hard drive and other computer related operation equipment, cameras/video cameras/web cameras, digital photographs, printers, electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media); and routers, modems, and network equipment used to connect to the Internet. (All items in this sub-paragraph are hereinafter referred to as "DEVICES");

a. Evidence of who used, owned, or controlled the DEVICES, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Any input/output peripheral devices, passwords, data security devices, and related security documentation that could be related to the DEVICES;

c. Evidence of software that would allow someone or something other than the user to control the DEVICES, such as viruses, Trojan horses, spyware, malware, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. Evidence of the lack of such malicious software on the DEVICES;

e. Evidence of software designed to protect the DEVICES from other persons, software, devices, or intrusions that may attempt to infiltrate, access, or control the DEVICES, such as pop-up blockers, security software, password protection, and encryption;

f. Evidence of other storage devices being attached to the DEVICES;

g. Evidence of counter-forensic programs and hard drive/computer cleaning programs (and associated data) that are designed to eliminate data from the DEVICES or frustrate the efforts of law enforcement to locate evidence on the DEVICES;

h. Evidence of the times the DEVICES were used;

i. Evidence indicating how and when the DEVICES were accessed or used to determine the chronological context of the DEVICES access, use, and events relating to crime under investigation and to the DEVICES' users;

j. Evidence of where the DEVICES were used, including evidence of wireless Internet networks and Internet Protocol addresses;

k. Passwords, encryption keys, and other access devices or programs that may be necessary to access the DEVICES;

l. Correspondence and contact information pertaining to counterfeit sports memorabilia or other counterfeit items;

m. Evidence indicating the DEVICES' user's state of mind as it relates to the crime under investigation;

n. Documentation and manuals that may be necessary to access the DEVICES or to conduct a forensic examination of the DEVICES;

o. Records of or information about Internet Protocol addresses used by the DEVICES;

p. Records of or information about the DEVICES' Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

q. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of the DEVICES found; and

r. Documents and records regarding the ownership and/or possession of the searched premises or DEVICES;

11. During the execution of the search of the locations identified in Attachment A, and for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant, law enforcement personnel are authorized to: (A) press BRYAN KENNERT'S fingers (including thumbs) to the Touch ID or fingerprint

sensor on any seized DEVICES; and/or (B) apply the facial recognition feature on any seized DEVICES to KENNERT.

Section II

The items identified in Section I shall be searched and seized to locate property, evidence, fruits, and instrumentalities of violations of 18 U.S.C. §1341 (frauds and swindles) and 18 U.S.C. §1343 (fraud by wire, radio, or television)

1. DEVICES determined on-scene not to contain items listed in Attachment B will be left at the subject premises. The remaining items will be seized and searched by forensic examination or further review off-site and will be returned as soon as reasonably possible if they are determined not to contain evidence listed in Section I of Attachment B.

2. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.